CLAIMS

1. A method of authorising data transfer to or from a mobile node temporarily connected to an attachment point of a network, the attachment point having a forwarding node associated therewith for forwarding messages to or from the mobile node, the method including the steps of:

(a) receiving a digital certificate from the forwarding node, which certificate includes a message body and a digital signature for verifying the content of the message body, the message body having geographical information therein, which geographical information is derived from a physical location;

(b) performing a comparison between the geographical information of the certificate and a further item of geographical information; and,

(c) making an authorisation decision for data transfer to or from the mobile node in dependence on the result of the comparison.

2. A method as claimed in claim 1, wherein the digital certificate is suitable for use in a public key encryption system

3. A method as claimed in claim 2, wherein the certificate is generated at a certificating node having a public key and a private key associated therewith, and wherein the signature is a function, at least in part, of the private key of the certificate node

4. A method as claimed in claim 2 or claim 3, including the step of verifying the authenticity of the digital certificate by performing a computation on at least part of certificate, the computation involving the public key associated with the certificate node.

5. A method as claimed in any of the preceding claims, wherein the mobile node has a certificate associated therewith, which certificate includes geographical information, the method including the further step of receiving the certificate from the mobile node, and using the geographical information from the certificate of the mobile node to make the authorisation decision.

6. A method as claimed in any of the preceding claims, wherein a registration procedure is performed to allow data transfer between the forwarding node and the mobile node, and wherein the registration procedure includes the steps of: receiving, at the forwarding node, a certificate with geographical information therein; and, comparing the received geographical information with a further item of geographical information.

7. A method as claimed in any of the preceding claims, wherein the geographical information in the certificate associated with the forwarding node is derived from the physical location of the forwarding node

8. A method as claimed in any of the preceding claims, wherein the mobile node has a temporary address and a permanent address associated therewith.

9. A method as claimed in claim 8, wherein the temporary address of the mobile node is indicative of the topological position of the current point of attachment of the mobile node.

10. A method as claimed in claim 8 or claim 9, including the steps of: (i) intercepting packets addressed to the permanent address of the mobile node; and, (ii) forwarding the intercepted packets towards the temporary address of mobile node, at least one of steps (i) and (ii) being authorised in dependence on the result of a comparison involving geographic information within a certificate.

11. A method as claimed in any of the preceding claims, wherein the forwarding node is a fixed node.

12. A method as claimed in any preceding claim, including an authentication step.

13. A network node for authorising the transfer of data to a mobile node temporarily connected to a forwarding node, wherein the network node is configured, in response to receiving a digital certificate from the forwarding node, to read at least part of the digital certificate, the digital certificate including geographical information derived from a physical location, and wherein the network node is further configured to: perform a comparison between the geographical information of the certificate and a further item of geographical

information; and, in dependence on the result of the comparison, make an authorisation decision.

14. A method of authorising data transfer to or from a mobile node using a digital certificate, wherein the digital certificate includes a message body, a digital signature for verifying the content of the message body, the message body having geographical information derived from a physical location, the method including the steps of: receiving the digital certificate from the mobile node; performing a comparison between the geographical information of the certificate and a further item of geographical information; and, making an authorisation decision in dependence on the result of the comparison.

15. A method as claimed in claim 14, wherein the mobile node is configured to form a temporary attachment to an attachment point of a main network, and wherein the digital certificate is received at a network node in the main network.

16. A method as claimed in claim 15, wherein the attachment point has a forwarding node associated therewith for forwarding messages to and/or from the mobile node, and wherein the forwarding node has a digital certificate associated therewith, which certificate include geographical information derived from the physical location of the forwarding node, the method including the steps of: at the network node, receiving the digital certificate from the forwarding node; and, making an authorisation decision in dependence on the geographical information of the certificate from the forwarding node.